IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Weller et al.

Attorney Docket No.: VISAP064P11500

Application No.: 09/842,313

Examiner: Unassigned

Filed: April 24, 2001

Group: Herewith

Title: ON-LINE PAYER AUTHENTICATION SERVICE

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail to: Assistant Commissioner for Patents, Washington, DC 20231 on May 25, 2001.

Printed Name: Agnes Spence

Signed: _____

PRELIMINARY AMENDMENT

Commissioner for Patents
Washington, D.C. 20231

Dear Sir or Madame:

For this preliminary amendment, which is intended to precede the first office action, please enter the following amendments and remarks:

06/01/2001 WKOROMA 00000033 09842313

01 FC:102 400.00 OP
02 FC:103 162.00 OP

Please **SUBSTITUTE** the following amended paragraph/section for the pending paragraph (a marked up copy of the prior pending paragraph with all changes shown is supplied in the appendix):

Please replace the pending paragraph, which begins on page 3, the 3rd full paragraph with:

In a second embodiment, the invention is directed towards the use of an integrated circuit card (also known as a smart card or chip card). One aspect of the second embodiment pertains to a method for authenticating the chip card being used by a customer. This method involves verifying that said cardholder client device includes a chip card reader and then prompting said cardholder to enter said chip card into the chip card reader. After the chip card reader receives the chip card, the chip card generates a cryptogram which is then sent to the access control server. The access control server then independently generates a second cryptogram based upon information in the chip card and compares the chip card cryptogram to the second cryptogram. If the two independently generated cryptograms match, then the authenticity of the card is verified.

Please replace the pending paragraph, which begins on page 9, the 1st continuing paragraph with:

The issuer domain 102 includes an enrollment site 108, an issuer cardholder system 110, the cardholder client device 122, an enrollment server 112, an access control server 114, an issuer or third party identity authentication component 116, and an account holder file 118. Optionally, the issuer domain 102 can include an issuer file of approved cardholders 120. The enrollment server 112 is a computer that manages cardholder enrollment into the PAS service through presenting a series of questions via a web interface to be answered by the cardholder and verified by the issuer. As shown in FIG. 1, the card issuer operates the enrollment server 112. However, a service organization, such as Visa, may operate the enrollment server 112 on behalf of the issuer. The issuer may use a web-enabled, interactive "identity authentication service" provided by a third party during the enrollment process to help validate a cardholder's identity. The enrollment server 112 is connected via the Internet to the Internet Payment Gateway Service 124, which is in turn, connected to a telecommunications network 126, for example, VisaNet.

The Internet Payment Gateway Service 124 allows the enrollment server 112 to communicate with the telecommunications network 126. The connection via the Payment Gateway Service 124 allows the enrollment server 112 to query the issuer's authorization system 138 to determine if a cardholder being enrolled has an active card account. Enrollment site 108 is an Internet web site where the cardholder can register to participate in the PAS.

Please replace the pending paragraph, which begins on page 12, the 2nd full paragraph with:

Before an Issuer can be set up to use PAS they must obtain a copy of all PAS software specified in the Issuer domain and install hardware systems and the PAS software. Then, Issuer financial institutions will also provide identity authentication policies and participating BIN information to PAS to be used in cardholder identity verification processes. Optionally, the issuer can provide to the PAS the cardholder authentication information for pre-loading into the account holder file 118. Pre-loading facilitates large volume support of cardholders. For example, when an issuer desires to activate all or most of its cardholders for PAS, the issuer can send PIN numbers to all of its cardholders. The PIN number can then be used by each cardholder to access his or her preloaded passwords. In this manner, the enrollment process is expedited because each cardholder need not go through the formal PAS enrollment process. After the cardholders use their preloaded password for the first time, the cardholders have the option of designating a new and easier to remember password.

Please replace the pending paragraph, which begins on page 15, the 2nd full paragraph with:

On the other hand, if the account number is determined to be within a range of account numbers present in directory server 128, then the second step of the verification process begins. The second step of the verification begins by the directory sending the ACS capable of authenticating the cardholder the card number to determine if the card is enrolled. If the card is not enrolled, the enrollment process is terminated. If the ACS indicates that the card is enrolled, the ACS via the directory server returns its URL Internet address to the merchant plug-in. The merchant plug-in then invokes the ACS via the cardholder client device and its resident browser. Once again it is noted that there can be multiple ACS's in PAS.

Please replace the pending paragraph, which begins on page 16, the 1st full paragraph with:

The payment authentication continues if the correct password is immediately entered or if the correct response is provided by the cardholder to the hint question within the allowed number of attempts. The ACS then proceeds to digitally sign a receipt using the issuer's signature key or a service provider's key. This receipt will contain the merchant name, card account number, payment amount, and the payment date. The receipt file 130 stores the following transaction data: merchant name, merchant URL, card account number, expiration date, payment amount, payment date, the issuer payment signature and the cardholder authentication verification value. The ACS then redirects the cardholder back to the merchant plug-in through the cardholder browser. At this point, the ACS also passes to the merchant the digitally signed receipt and the determination as to whether the cardholder has been authenticated. The validation server 136, in the acquirer domain 106, is used by the merchant plug-in 134, to verify the digital signature used to sign the payment receipt. After verifying the digital signature, the cardholder is deemed "authenticated." In some embodiments of the invention, after the transaction is completed, the cardholder will also have the ability to re-register his or her card account and create a new password to be used for future online purchases.

Please replace the pending paragraph, which begins on page 21, the start of the 3rd paragraph with:

In the case that the acquirer domain 106 contains a validation server, the validation server 136 validates the signature on the *PARes*. The validation server 136 then returns the result of the signature validation to the merchant plug-in. On the other hand, if the signature is validated, the merchant proceeds with an authenticated payment authorization. The *PARes* message may also be passed from the merchant to its acquirer payment processor 140 as shown in line 6a. The *PARes* message may then be passed from the acquirer through a telecommunications network 142 to the issuer. Thus, the payer authentication results are made available to the issuer as part of the standard payment authorization process.

Please replace the pending paragraph, which begins on page 25, the start of the 3rd full paragraph with:

In a second technique, the PAS password is automatically supplied to the ACS by the chip card. This technique uses passwords stored on the chip card to authenticate the cardholder in order to allow the cardholder to utilize the chip card. This approach uses an applet resident on the card referred to as the "Access" applet, because it provides universal access to the card and its resident applications, and can be used to authenticate a cardholder. The Access applet can also disable access to the applications on the card. Upon presentation of the single, universal "Access" password and authentication of the cardholder, the Access applet then allows the cardholder to access to a variety of services or applications (e.g., access to an online banking site, access to an electronic bill payment service). For example, by presentation of a single "Access" password, the applet then allows use of any stored passwords on the card.

Please replace the pending paragraph, which begins on page 25, the start of the last paragraph with:

Generally, the set up procedures and the authentication process for the chip card embodiment are the same as for the traditional card embodiment. The differences between the chip card embodiment and the traditional card embodiment will be evident in the description that follows.

Please replace the pending paragraph, which begins on page 26, the 2nd full paragraph with:

FIG. 10A provides a high-level system architecture view of one embodiment of the chip card payer authorization service. As usual, the payment transaction begins when the cardholder accesses a merchant's electronic commerce web site using a cardholder client device 122. The cardholder client device 122 contains a chip payer authentication client plug-in 1542 and is connected to the issuer access control server 114, which has a chip payer authentication ACS plug-in 115. The issuer ACS 114 is connected to an account holder file 118, which is in turn connected to a receipt file 130. The merchant 132 uses a merchant plug-in software module 134 to participate in the payer authentication service. The merchant 132 is connected to the directory

server 128, the validation server 136, and the acquirer payment processor 182. The acquirer payment processor 182 is connected to the payment network 126, which is in turn connected to the issuer 180.

Please replace the pending paragraph, which begins on page 27, the 3rd full paragraph with:

Now, FIG. 12 is presented to illustrate payment process flows that are superimposed upon a chip card system architecture according to one embodiment of the present invention. The chip card authentication architecture 1500 involves the cardholder client device 1510, the issuer's ACS 1520, the cardholder 1530, the chip card 1540, and the requesting party 1550. The requesting party in the PAS environment is typically the merchant. The cardholder client device 1510 includes a display device 1512, terminal software 1514, PIN pad or key entry device 1516, and the card reader 1518. The card reader 1518 is the electromechanical device into which a chip card is inserted for use with a terminal application, functionally equivalent to a Card Acceptance Device or InterFace Device (IFD in a physical point of sale environment).

Please replace the pending paragraph, which begins on page 30, the 3rd paragraph, line 16 with:

This section briefly describes the phases of the VSDC Authentication processing in the order in which they occur as illustrated in FIG. 12A: